Appendix A:

DISA Instruction 630-230-19, Automated Data Processing – Information Systems Security Program.

DISA INSTRUCTION 630-230-19*

AUTOMATIC DATA PROCESSING

Information Systems Security Program

1. Purpose. This Instruction prescribes policy and assigns responsibilities for implementing, managing, and maintaining the DISA Information Systems Security Program.

2. Applicability. This Instruction applies to DISA; the Office of the Manager, National Communications System (OMNCS); indi-viduals who use, design, operate, and manage DISA information technology; and companies or individuals contracted to perform information system services on behalf of DISA, on DISA premises, or at contractor sites.

3. Authority. This Instruction is published in accordance with the authority contained in DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, 8 February 1996; and Public Law 100-235, Computer Security Act of 1987, 8 January 1988.

4. References.

a. DoD 5200.1-R, Information Security Program Regulation, June 1986.

b. DISAI 240-110-8, Information Security Program, 24 June 1996.

c. OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, 9 July 1990.

5. Definitions. Definitions for terms used throughout this Instruction immediately follow the table of contents.

*This Instruction cancels DISAI 630-230-19, 28 August 1991; Supplement 1 to DISAI 630-230-19, 27 April 1994; and Supplement 2 to DISAI 630-230-19, 27 April 1994.
(For Summary of significant changes, see signature page.)
OPR: CIO
Distribution: A, B, J

6. Scope. This Instruction is limited to a discussion of three major areas: certification and accreditation, compliance, and information systems security awareness and professionalization training of DISA users and of those individuals assigned to manage the implementation of the DISA Information Systems Security Program. Information technology, as referred to in this Instruction, includes major applications; general support, communications, and network systems; operating system software (e.g., executive software); and other information technologies, as they may be developed. Information technology that has been assigned to DISA to manage and operate, but is governed by external policies, shall also be protected in accordance with (IAW) the intent of this Instruction.

7. Background. The DISA Information Systems Security Program establishes a standardized oversight structure to ensure that adequate security is provided for all DISA information collected, processed, transmitted, stored, or disseminated by DISA infor-mation technology. On 20 October 1994, DISA centralized the responsibilities of the Designated Approving Authority (DAA) and the Certification Authority with the Chief Information Officer (CIO) and with the Commander for the Center for Information System Security (CISS), respectively.

8. Policy.

a. Information Protection. DISA information will be protected from unauthorized disclosure, destruction, or modi-fication while collected, processed, transmitted, stored or disseminated.

b. Risk Management. The principles of risk assessment and mitigation will be used to ensure that organizations assess, reduce, and continually manage the risks to DISA information regardless of the technology used and to select and implement those countermeasures which effectively satisfy the requirements of confidentiality, integrity, and availability.

c. Use of Trusted Computer Products. Information systems that process classified and/or sensitive but unclassified information will comply with the minimum requirements for controlled access protection. The implementation of controlled access protection or more stringent security features will be evaluated in operational environments to assess protection effectiveness. In instances where the introduction of controlled access protection is technically unsound or adversely impacts operational effectiveness, the Office of Primary Responsibility (OPR) of the General Support System or the Functional Application may request an exception to implementation of this policy.
In cases where exceptions are requested, other safeguards may be substituted as long as the requisite level of security
is maintained (e.g., physical, administrative, or procedural controls).

d. Accreditation. All DISA information systems will be accredited to operate IAW a set of security safeguards formally approved by the DAA.

e. Access by Foreign Nationals. All requests for foreign national access to a DISA information system shall be adjudicated by the Director, DISA, or duly authorized representative.

f. Fraud, Waste, and Abuse. DISA information systems will be used only in an official capacity in support of the DISA mission. DISA employees will use only government-developed or government-approved/purchased hardware and/or software to perform government business in the office. Personally owned hardware or software will not be used in the official conduct of government business nor will it be installed on DISA information assets for personal use or gain. Additionally, use of entertainment and games software is prohibited. When expressly permitted to work at home, personally owned hardware and/or software may be used. However, when permitted to work at home, such approval must specifically establish the conditions under which permission is given and provide guidance regarding system use and security (particularly if the user is processing sensi-tive but unclassified information).

g. Communication Links. Classified information shall be protected during transmission by approved National Security Agency (NSA) methods. Sensitive but unclassified information shall be protected during transmission in a manner commensurate with the level of risk and magnitude of loss or harm that could result from disclosure, loss, misuse, alteration, destruction, or nonavailability.

h. Acquisitions. Security requirements for systems that process classified and sensitive but unclassified information shall be identified prior to purchase of equipment or services. These security requirements will be included in Statements of Work (SOW), requests for proposals, contracts, and other similar acquisition documents.

i. Information Systems Security Awareness and Training. In compliance with the authority document, Computer Security Act of 1987, DISA requires mandatory periodic training in computer security awareness and accepted computer security practices for all personnel having access to government information systems including contractors, employees of other agencies, and members of the public.

j. Malicious Code. It will be considered a major security violation for any DISA employee or contractor to deliberately introduce malicious logic or computer viruses into any DISA information system. It is also a violation to withhold information necessary for effective implementation of countermeasures or antivirus procedures.

k. Copyright and Licensing. Purchased and/or licensed software will be used IAW the vendor's established copyright or license provisions. DISA personnel or individuals contracted to provide information technology services may be held liable for any infringement of copyrighted software licensing agreements.

l. Privately Owned Computers. The use of privately owned computers (those not owned or leased by DISA or a DISA contractor) to process classified information is absolutely prohibited.

m. Position Sensitivity Designation. Information System Security Officials and System Administrator positions will be designated as ADP-I and investigated according to the require-ments described in DoD 5200.2-R, Personnel Security Program, January 1987.

n. Functional Application Office of Primary Responsibility. Each Major

Application will have an identified Functional Application OPR. In those cases where a Functional Application OPR cannot be determined, the DAA will assign responsibility,
as necessary.

o. General Support System Office of Primary Responsibility. Each General Support System will have an identified General Support System OPR. In those cases where a General Support System OPR cannot be determined, the DAA will assign respon-sibility, as necessary.

p. System Security Plans (SSPs). An SSP shall be developed for each DISA Major Application and General Support System. (Guidance for developing SSPs is provided in chapter 3 of this Instruction.)

q. Systems Planning and Design. Activities that plan and design information systems shall have adequate internal controls that provide reasonable assurance that the recording, processing, and reporting of data are properly performed during operation
of the information system and that they conform with applicable security regulations, policy, and requirements, as stated in
the authority document DoDD 5200.28 and the DoD Technical Architecture Framework for Information Management (TAFIM),
Volume 6, DoD Goal Security Architecture, 30 June 1994.

9. Responsibilities. Responsibilities for performing informa- tion systems security duties are delineated in chapter 1.

FOR THE DIRECTOR, DISA, AND MANAGER, NCS:

A. FRANK WHITEHEAD
Colonel, USA
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES. This document represents a significant revision and should be reviewed in its entirety. This Instruction has been refocused to provide policy and assign responsibilities for implementation. This Instruction adopts the terminology used in the recently promulgated authority document OMB Circular A-130 to redefine information technology as either major applications or general support systems and includes new requirements to achieve "adequate security."

PAGE INTENTIONALLY LEFT BLANK

CONTENTS

ILLUSTRATIONS

Figure | Page

Table | Page

DEFINITIONS

Automated Information System (AIS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. This includes standalone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; embedded computer systems; communications switching computers; personal computers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies as may be developed.

Clearing. Clearing is the removal of the pointer to data, so that the system will place that storage space back into the usable arena and overwrite it as the system requires. There is a reasonable level of assurance that the data may not be reconstructed using normal system capabilities, (e.g., through the keyboard). An information system need not be disconnected from external networks prior to clearing. Media cannot be declassified when clearing methods are used, and cleared media must remain safeguarded, controlled, and marked commensurate with the highest classification of information ever recorded thereon.

Declassifying. Declassifying is a procedure and an administrative decision to remove the security classification of subject media. The procedural aspect of declassification is the actual purging of the media and removing of all labels denoting original classification category. Relabeling may be required. Collateral classified media may be declassified if purged in accordance with National Computer Security Center NCSC-TG-025, A Guide to Understanding Data Remanence in Automated Systems, September 1991. Declassifying is required when media will be released outside the facility, such as when equipment is turned in for repair, excessed, or released to another facility, agency, or activity.

Degauss. The reduction of magnetic flux density to zero by applying an electrical devise that can reverse a magnetizing field.

General Support System. A General Support System is an interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, or a communications network. Normally, a General Support System provides processing or communications support.

Individual Accountability. The ability to associate positively the identity of a user with the time, method, and degree of access to a system.

Information System. The terms information system and automated information system (AIS) are interchangeable.

Infraction. Any knowing, willful, or negligent action contrary to the standards or requirements of Executive Order 12958, Classified National Security Information, 17 April 1995, or its implementing directives that does not comprise a violation.

Major Applications. A Major Application is an application (to include the information and the information technology used to satisfy a specific set of user requirements) that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A Major Application may be operating on an information system designed specifically for its support or it may be part of a General Support System. While a multitude of applications are used throughout DISA on a daily basis, certain applications, because of the sensitivity of information processed, require special management oversight and should be treated as Major Applications.

Periods Processing. A manner of operating an automated information system in which the security mode of operation and/or maximum classification of data handled by the automated system is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the automated information system to the completion of any purging of sensitive data handled by the automated information system during the period.

Purging. Purging is the removal of sensitive data from an information system (including storage devices and other peripheral devices with storage capacity) at the end of a period of processing in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed through open-ended laboratory techniques. An information system must be disconnected from any external networks before purging.

Risk Management. The total process of identifying, measuring, and minimizing uncertain events affecting information system resources.

Security Modes of Operation. A description of the conditions under which an information system functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users. DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988, identifies the following four modes of operation:

- Dedicated Mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the information system. If the information systems process special access information, all users require formal access approval. In the dedicated mode, an information system may handle a single classification level and/or category of information or a range of classification levels and/or categories.

- System High Mode. A mode of operation wherein all users having access to the information system possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the information system. If the information system processes special access information, all users must have formal access approval.

- Multilevel Mode. A mode of operation that allows two or more classification levels of information to be processed at the same time within the same system when not all users have a clearance or formal access approval for all the data handled by the information system.

- Multilevel, Partitioned Mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the information system. This security mode encompasses the compartmented mode defined in the Director of Central Intelligence Directive Number 1/16, Security Policy on Intelligence Information in Automated Systems and Networks (U), 4 January 1983.

Users. Users are people or processes accessing an information system either by direct connections or indirect connections.

Violation. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; or any knowing and willful action to classify or continue the classification of information contrary to the standards of the Executive Order 12958, Classified National Security Information, 17 April 1995, and its implementing directives.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1. PROGRAM ROLES AND RESPONSIBILITIES

1. General. The DISA Information Systems Security Program identifies and establishes the policies, roles, and responsibilities necessary to ensure that adequate security is provided for DISA information and information technology. Adequate security is defined as: "Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Adequate security also includes ensuring that all DISA systems and applications operate effectively and that they provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

2. Program Goal. The goal of the DISA Information Systems Security Program is to merge information, personnel, physical, communications, computer, industrial, emanations, and procedural security disciplines into a single program focused on providing protection that is commensurate with known threats and the value and mission criticality of the information and information technology based on the known threat(s).

3. Objective of Instruction. This Instruction supports the program goal by:

a. Identifying roles and assigning responsibilities for the implementation of the DISA Information Systems Security Program.

b. Defining comprehensive and integrated security requirements necessary to obtain management authorization (accreditation) to allow DISA information technology to operate in a particular security mode and within an acceptable level of operational security risk.

c. Providing a basis for implementing a security awareness and professionalization training program that ensures all individuals are aware of their security responsibilities and trained in how to fulfill those responsibilities.

4. Program Management. The DISA Information Systems Security Program shall be managed by the office of the Chief Information Officer (CIO). The CIO Information Systems Security Program Management Division is responsible for effective implementation of this Instruction at DISA activities worldwide. CIO will prepare, promulgate, and approve supplemental policies to this Instruction as they are developed.

5. Program Support. The effectiveness of the DISA Information Systems Security Program is reliant upon all DISA personnel being

familiar with their roles and responsibilities. Therefore, program responsibilities must be shared by users of DISA information technology and by those responsible for planning, managing, and implementing their respective facets of the DISA Information Systems Security Program.

6. Delegation of Authority. Per authority document, DoD Directive 5200.28, the Director, DISA, is responsible for implementing, maintaining, funding, and providing adequate resources for the DISA Information Systems Security Program. To ensure that the program receives effective management oversight, the Director, DISA, has designated the CIO as the sole Designated Approving Authority (DAA) for all DISA information systems. Additionally, the Center for Information Systems Security (CISS) has been designated as the sole DISA Certification Authority.

7. Security Management Roles and Responsibilities.

a. Designated Approving Authority (DAA). The DAA is the appointed management official tasked to determine the level of acceptable risk. The DAA is also the official tasked to authorize the operation of an information system once an acceptable level of risk has been obtained. If the level of risk is deemed acceptable, the DAA is responsible for issuing an accreditation statement. The accreditation statement indicates that the DAA formally accepts security responsibility for the operation of the system and officially declares that the specified system is adequately protected against compromise, destruction, or unauthorized modification under stated parameters of the accreditation. The DAA shall:

(1) Review and approve security safeguards, ensure that each information system is properly accredited based on its environment and sensitivity levels, and issue written accreditation statements.

(2) Ensure an effective information system security education, training, and awareness program is in place.

(3) Ensure that data ownership is established for each information system, to include accountability, access rights, and special handling requirements.

(4) Take action, where the Certification Authority has recommended a denial to accredit, to achieve an acceptable security level (e.g., allocate additional resources).

(5) Appoint a Component Information System Security Manager (CISSM).

(6) Periodically brief the Director, DISA, regarding unresolved issues relating to the accreditation of DISA information technology and other programmatic information security issues.

b. Component Information System Security Manager (CISSM). The CISSM manages the DISA Information Systems Security Program on behalf of the DAA. The CISSM is responsible for coordinating the effective use of security related resources to include the development and promulgation of cost-effective approaches to securing information technology and for providing centralized enforcement and oversight of the security program. In addition to the development of centralized security policy, the CISSM functions as the representative to the DAA and, as such, provides the DAA with analyses of threats to DISA information technology. The CISSM shall:

(1) Develop and promulgate policy, consistent with existing information systems security directives, laws, and guidelines, to establish the DISA Information Systems Security Program and assign responsibility for its implementation.

(2) Develop and administer the DISA Information System Security Program and coordinate the effective use of security related resources throughout DISA.

(3) Establish a risk management program to identify, assess, and mitigate risk while recognizing that information technology will never be fully secured.

(4) Maintain a record of security related incidents and violations and report serious unresolved violations to the DAA and to the DISA Inspector General.

(5) Establish an oversight program to address compliance with DISA-specific information systems security requirements as well as national requirements prescribed under authority documents OMB Circular A-130 and Public Law 100-235.

(6) Report to the DAA the status of DISA information systems security and training programs and actions required to improve security.

(7) Ensure that qualified Information Systems Security Managers (ISSMs) are appointed.

c. Certification Authority. The Certification Authority is responsible for ensuring that information system security policy is satisfied through technical and nontechnical evaluations of system compliance with stated requirements. The Certification Authority is responsible for conducting certification activities in support of the accreditation process. The Certification Authority's final report is used by the DAA in forming an accreditation decision. The Certification Authority will:

(1) Ensure security testing and evaluation is completed and documented IAW the DAA-defined information system security program goals.

(2) Maintain certification-specific accreditation documentation.

(3) Provide the DAA with written recommendations for accreditation.

(4) Periodically review required safeguards as approved and identified in the accreditation documentation and ensure that the safeguards have been implemented and maintained via the compliance validation process.

(5) Identify security deficiencies and, where the deficiencies are serious enough to preclude accreditation, make recommendations to assist the organization in attaining an acceptable level of security.

d. Deputy Directors, Headquarters, DISA; Commanders and Chiefs of DISA Field Activities; and the Deputy Manager, NCS. These individuals are responsible for overall management, implementation, and compliance for areas under their control. While they do not perform the functions of the DAA, they are still responsible for providing appropriate security, including management controls, operational controls, and technical security controls, using the principles of risk management. These individuals perform the initial steps of risk management by ensuring that an adequately trained information system security infrastructure exists within their organizations to effectively implement the policies and requirements prescribed in this Instruction. These individuals will:

(1) Appoint an organizational ISSM and subordinate ISSMs, as necessary. Where the organization does not have responsibility for major applications (i.e., mission support or mission critical) or are not considered General Support System providers, they may consider the necessity of sharing this responsibility with organizations of similar size and information technology complexity.

(2) Ensure that organizational personnel are aware of their responsibilities under the program and that they participate in appropriate information security training programs.

(3) Ensure that appropriate, timely, and cost-effective information systems security safeguards are implemented within all of their organization's information systems (i.e., mission support, mission-critical, general support systems) in preparation for the activities of certification and accreditation.

8. Security Staff Roles and Responsibilities.

a. Information System Security Manager (ISSM). The ISSM is the focal point for all organizational information systems security concerns and ensures that the program requirements described in this Instruction are implemented. The ISSM must possess knowledge of the organization's mission, mission information sensitivity, and information technology to ensure that the program requirements described in this Instruction are met. The ISSM implements the overall information system security program for an organization and should not participate in daily information system operations. The ISSM will:

(1) Assess the organization's information technology complexity and ensure an adequate information system security infrastructure is in place to implement the day-to-day security program requirements. (The infrastructure may consists of an Information System Security Officer (ISSO) for each information system, a Network Security Officer (NSO) for networks not controlled, managed, or operated by the General Support System provider, and sufficient Terminal Area Security Officers (TASOs) for terminal groups operating in a standalone mode.)

(2) Ensure that organization information technology is operated within an acceptable level of risk and are accredited.

(3) Ensure that all information systems security related incidents and violations are immediately reported, properly investigated, and correctly resolved.

(4) Ensure that all changes to information systems or the security infrastructure are evaluated from a security viewpoint.

(5) Ensure that security plans for systems that process sensitive but unclassified, and classified information, are developed consistent with chapter 2 of this Instruction.

(6) Review and approve security specifications for acquisition of the organization's information technology.

b. Information System Security Officer (ISSO). An ISSO will be appointed for each information system or group of information systems that support the mission of the organization. The ISSO acts on behalf of the CISSM to ensure compliance with the information system security procedures developed for the local environment. The same ISSO may be appointed for multiple information systems, local area networks, or small systems or workstations that provide automated technical security controls for individual accountability, access control, and auditing. Within an organization, the ISSO may be one or more individuals who have the responsibility to ensure the security of an information system. "ISSO" does not necessarily refer to the specific functions of a single individual. ISSOs who function as System Administrators will be provided sufficient information security training to effectively administer the information systems under their cognizance. Where the ISSO responsibilities have been contracted out, the Deputy Director, Commander, Chief, or Program Manager will designate a responsible government individual to oversee the "contractor" ISSO. ISSOs are responsible to the DAA for maintaining the approved accredited baseline. ISSOs will:

(1) Ensure that information systems under the ISSO's cognizance are operated, managed, secured, and used IAW internal security policies and procedures.

(2) Ensure that information systems under the ISSOs cognizance are accredited according to this Instruction.

(3) Ensure that users and operations personnel have the appropriate personnel security investigations, clearances, need-to-know, and authorization and that they are aware of their security responsibilities as they relate to the security of the information systems they access.

(4) Review audit records and report any deviation of security practices to the ISSM.

(5) Prepare, maintain, and distribute plans and system-specific security guidance regarding the technical security controls implemented in the information system over which the ISSO has oversight.

(6) Report security incidents IAW site specific requirements for reporting computer security incidents and violations.

(7) Maintain the information systems accredited baseline according to the statement of accreditation. For information systems that have been accredited, annually evaluate the accredited baseline and document the result of the evaluation. For an information system that has been issued an Interim Authority to Operate (IATO), ensure that the plan approved for making system security improvements progress toward meeting the requirements to obtain accreditation.

c. Network Security Officer (NSO). An NSO will be appointed for each identified network and will implement the Information System Security Program for all networks within their purview. The NSO's responsibilities are similar to those of the ISSO, with the NSO concentrating on network security and the ISSO concentrating on information system security. Depending on the size and complexity of the information system, the NSO may also be the ISSO. NSOs will:

(1) Ensure compliance with information system security procedures for the network.

(2) Develop, maintain, and distribute plans, guidance, procedures, and instructions concerning security of the network.

(3) Review and evaluate the security impact of changes to the network, including interfaces with other networks.

d. Terminal Area Security Officer (TASO). TASOs will be appointed for each workstation or contiguous group of work-stations operating in a standalone mode. TASOs are responsible for overseeing the information system security procedures in an assigned area. TASOs may be assigned security responsibility for multiple workstations or areas as long as the ISSM/ISSO is satisfied that security is being maintained. If the TASO can logically maintain security control over multiple workstations in different rooms, then the intent of this requirement is met. TASOs will:

(1) Monitor local compliance with security procedures.

(2) Implement access management and other security related functions within the scope of their assigned authorities.

(3) Report actual or suspected security deviations to the system ISSO.

9. Supporting Roles and Responsibilities.

a. Functional Application OPR. Each Major Application shall have an identified Functional Application OPR. Each OPR will define minimum security requirements that address accountability, access rights, special handling, confidentiality, integrity, and availability requirements of the Major Application under their cognizance. Functional Application OPRs shall provide for appropriate security, to include management, operational, and technical security controls. Functional Application OPRs shall also prepare a statement regarding the security integrity of the application and provide this statement to the OPR for General Support Systems.

b. General Support System OPR. Each General Support System that processes or operates a Major Application shall have an identified OPR. These OPRs will ensure the proper use of information technology and will implement the technical security controls that relate to the environment over which they have cognizance. The OPR will also establish minimum system requirements to include identifying system interfaces and product compatibility requirements. The General Support OPR will:

(1) Establish system-specific policy regarding the proper use of DISA information technology resources and will specify administrative sanctions for the misuse, abuse, and waste of these resources.

(2) Develop a set of system-specific rules to achieve adequate security. As a minimum, rules should include proper use of system privileges, sanctions regarding the unofficial use of DISA information technology, use of personally-owned software and hardware, connection to the INTERNET, dial-in access, and protection of system authenticators (e.g., smart cards, passwords).

(3) Provide security awareness training regarding the technical security features, system privileges, and security capabilities of general support applications made available for use. (Security awareness training will be made available prior to user access and offered within defined periodic intervals or, as a minimum, annually.)

(4) Establish a process to detect, eradicate, and report computer viruses; to identify and handle malicious code; and to describe events or conditions that may result in system penetrations by unauthorized individuals.

c. System Developers. System developers that are responsible for acquiring, developing, or integrating information systems shall ensure that these systems are accreditable. System developers shall ensure that the requirements outlined in this Instruction, and the specific requirements established by the Functional Application OPRs, are incorporated into the systems during the development process. System developers will designate responsible individuals to oversee the security aspects of the acquisition, development, and integration of the information system IAW the DOD Technical Architecture Framework for Information Management (TAFIM), Volume 6, DOD Goal Security Architecture.

d. System Administrators. System Administrators are responsible for the daily monitoring and maintenance of system access and resources. The number of required System Administrators can best be determined by identifying the length of time it would take to perform the duties and who has the most technical knowledge in operating systems and security software. System Administrators are unique in the fact that they can normally access all data stored or processed on the information system and are, therefore, likely candidates to act as the system ISSO. In those instances where the System Administrator does not function as the ISSO, the System Administrator will perform the following information system security functions:

(1) Assist the ISSO to ensure that the information system is being operated and used in a secure manner.

(2) Assist the ISSO in developing an information system security incident reporting program.

(3) Assist the ISSO in maintaining configuration control

of the systems and applications.

(4) Advise the ISSO of security anomalies or vulnerabilities associated with the information system and provide a potential means for fixing the identified vulnerabilities. Participate in the information system security incident reporting program.

(5) Administer, when applicable, user identification or authentication mechanisms of the information system or network.

e. Users. Users of DISA information systems will:

(1) Access DISA information systems only when formally authorized to do so and only for authorized purposes.

(2) Not disclose, lend, or otherwise compromise their personal authenticators (e.g., passwords).

(3) Promptly report any suspected compromise of their (or any other) authenticator to their TASO or ISSO.

(4) Comply with all information security requirements identified by cognizant security staff and recognize that deliberate failure to obey the security provisions of this Instruction may result in disciplinary action.

(5) Notify the TASO or ISSO when access to an information system is no longer required.

f. Supporting Organizations.

(1) The Deputy Director for Personnel and Manpower (D1) shall establish, with the assistance of the CISSM and CISS, an information systems security awareness and professionalization program. (The program shall provide for the continual systems security awareness of DISA users and for the continued professionalization of the individuals appointed to information systems security positions.)

(2) The Commander, CISS, shall assist the CISSM and the D1 Human Resources Development Branch (D113) in identifying training sources for the professionalization of DISA information system security professionals and in the development of automated cost-effective information systems security training tools for DISA users.

CHAPTER 2. SECURITY REQUIREMENTS

Section A. DESCRIPTION

1. General. This chapter discusses the various security disciplines and their required application in the DISA information technology environment. Section B identifies the minimum security controls necessary to enhance an organization's information system security processing environment, thereby creating the needed minimum security standardization. Section C specifically addresses security requirements that apply to Major Applications and/or General Support Systems. Major Applications and General Support Systems, as identified in authority document OMB Circular A-130, are the standard system types used throughout DISA.

2. Statements of Compliance. Prior to the commencement of certification, each organization will submit a statement of compliance with the minimum security requirements described below. Organizations will request exception to implementation where compliance has not been achieved. Periodic efforts to validate compliance may occur at random intervals at the request of the DAA.

3. Exceptions to Implementation. Exceptions to the implementation of the minimum security requirements must be approved by the DAA. Each request must justify the reason why the system cannot comply with stated minimum requirements and identify the supplementary countermeasures that have been implemented. Exceptions which affect the protection of a Major Application will be coordinated through the Functional Application OPR. All of the exceptions will be forwarded to the DAA through the appropriate management chain.

Section B. MINIMUM SECURITY REQUIREMENTS

4. General. All information systems regardless of classification or sensitivity will achieve compliance with the minimum security requirements described in this Section. Information systems that process nonsensitive information will be safeguarded from tampering, loss, and destruction, thereby safeguarding the DISA investment from fraud, waste, and abuse. Minimum security requirements for information systems processing nonsensitive information are indicated with an "*" following the subparagraph heading.

a. Access Controls. An access control policy will be developed to describe features and procedures for controlling and enforcing access to an information system. Access requests to information systems by foreign nationals can only be approved by the Director, DISA, or a designated representative. The following conditions must be met prior to granting access to a foreign national:

(1) No classified information is processed on the information system and it is not connected to other systems that process classified information.

(2) The foreign national is a resident alien of the United States, has been in resident alien status for at least the most recent 5 consecutive years, and has been subjected to a Background Investigation or National Agency Check.

b. Accountability. Safeguards will be implemented to ensure each individual having access to an information system may be held accountable for his or her actions while using the system. An audit trail will be used to provide a documented history of information system use and record information in sufficient detail to permit a reconstruction of events should a security compromise or incident occur. As a minimum, the audit trail will record the identity of the user, time of access, interaction with the system, and sensitive functions that might permit a user or program to modify, bypass, or negate security safeguards. The use of audit trails is left to the discretion of the DAA for standalone, single user computer systems that process nonclassified information.

c. Accreditation.* DISA information systems will be accredited to operate IAW a DAA approved set of security safeguards. Information systems that process classified information will be certified and accredited prior to commencement of operations.

d. Administrative Security Controls. Controls will be established to effectively operate an organization's information systems security program. Specifically identified are supplemental controls used in the management, operation, and use of information systems.

(1) Standard Security Operating Procedures. Documentation will be maintained that describes how security will be managed and will include rules for gaining both physical, local, and remote access. Additionally, procedures for providing local and remote access by maintenance personnel, and site specific rules for managing automated security management systems or access control programs will be documented. Standard security operating procedures include the development and review of audit trails, management of user identification codes (USERIDs) and passwords, and retention periods of information system security records.

(2) Information System Security Records. As a minimum, either the site ISSM or local ISSO will retain automated or hardcopy records regarding system access, violations or security

incidents, and Statements of Accreditation. Letters of appointments for ISSOs, TASOs, and NSOs, and documents relating to the conduct of security awareness training will also be retained. Audit trail records must be retained for a period that meets or exceeds the most stringent retention requirements applicable to information on the system being protected by the audit trail. In cases where specific data or audit record retention requirements do not exist, audit records will be retained for a period of at least 1 year.

(3) System Access Management Procedures. Access control procedures will ensure that access permissions can be justified for personnel who satisfy one or all the following criteria: a successfully adjudicated security clearance or level of security investigation appropriate for either access to classified or sensitive but unclassified information, formal access approval from the OPR of the respective Major Application, need-to-know approval from supervisor of the user, or as a result of being assigned to an appropriate ADP sensitivity designation (i.e., ADP-I, ADP-II, or ADP-III).

(4) Individual Accountability and Password Management. Criteria will be established to positively identify each user authorized access to the system. The granularity of the identification shall be sufficient to support audit trail requirements. In addition to the individual assignment of unique identifiers, guidelines must be established for the management of primary authenticators (e.g., passwords). As a minimum, passwords will be a minimum of six characters and changed at least every 180 days or more frequently as warranted. Passwords should be protected from disclosure and handled and marked as "FOR OFFICIAL USE ONLY." Passwords for systems that process classified information in the multilevel mode of operation, where the password is the only measure separating users from different levels of classified information, must be classified to the level of that user and protected accordingly.

e. Availability. Safeguards used by the information system must provide a level of availability commensurate with information system access control policy and all elements of the information system must function in a cohesive, identifiable, and predictable manner.

f. Communications Security Controls. Controls will be established to deny unauthorized persons from receiving information derived over telecommunication lines or from equipment. Established measures and controls must also ensure the authenticity of communication transmissions. Further guidance can be found in DISAI 240-115-3, Communications Security, 23 July 1992. For the purposes of this Instruction, communications security requirements are outlined below.

(1) Telecommunications paths transmitting classified

information will be secured by either NSA endorsed equipment and keying material or by Protected Distribution Systems (PDSs).

(2) Telecommunications paths transmitting sensitive but unclassified information will be protected in a manner commensurate with the level of risk and magnitude of harm that could result from unauthorized disclosure, loss, misuse, alteration, destruction, or nonavailability.

g. Confidentiality. Plans and procedures will be established to implement the required automated and manual controls to ensure the confidentiality of classified and/or sensitive but unclassified information.

h. Contingency Planning. Plans will be established to ensure the continuity of information processing support in the event of a disruption of service. Contingency plans will be developed and periodically tested IAW authority document OMB Circular A-130 to ensure that the information systems security controls function reliably and can be maintained continuously during interrupted service. Procedures must be in place for recovery if data is modified or destroyed.

i. Emanations Security Controls. Where required, controls will be established to deny unauthorized persons from receiving information of value that might be derived from interception and analysis of compromising emanations.

j. Guidance for User Behavior. DoDD 5500.7, Standards of Conduct, 30 August 1993, states that government assets will be used for the conduct of official government business. Therefore, organizations are responsible for developing specific guidance consistent with the use of technology purchased in support of their mission. Guidance should be as stringent as necessary to provide adequate security, clearly delineate security responsibilities, and define expected behavior for all individuals with access to this technology.

k. Information Security Controls. Controls will be established to identify, control, and protect information, particularly classified information, from unauthorized disclosure. Controls will also be established for the clearing, purging, and declassification of information stored on media used for classified processing. The process is described in the National Computer Security Center NCSC-TG-025, A Guide to